

STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2026-042
November 2025

UNIVERSITY OF FLORIDA

Oracle PeopleSoft Enterprise Applications



Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period June 2024 through May 2025, Dr. Kent Fuchs served as Interim President of University of Florida and the following individuals served as Members of the Board of Trustees:

Morteza "Mori" Hosseini, Chair	James W. Heavener
Rahul Patel, Vice Chair	Sarah D. Lynne ^b
David L. Brandon	Daniel T. O'Keefe
John E. Brinkman through 4-21-25 ^a	Marsha D. Powers
Richard P. Cole	Fred S. Ridley
Christopher T. Corr	Patrick O. Zalupski
Blake E. Cox from 4-22-25 ^a	Anita G. Zucker through 2-19-25
Jed V. Davis from 2-20-25	

^a Student Body President.

^b Faculty Senate Chair.

The Auditor General conducts audits of government entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

The team leader was Joseph Clayton and the audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Heidi Burns, CPA, CISA, Audit Manager, by e-mail at heidiburns@aud.state.fl.us or by telephone at (850) 412-2926.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

UNIVERSITY OF FLORIDA

Oracle PeopleSoft Enterprise Applications

SUMMARY

This operational audit of the University of Florida (University) focused on evaluating selected information technology (IT) controls applicable to the Oracle PeopleSoft Enterprise Applications and the University's IT infrastructure and included a follow-up on the findings included in our report No. 2019-138. Our audit disclosed the following:

Finding 1: University security awareness training needs improvement to reduce the risk that University data will be compromised.

Finding 2: Certain University IT security controls related to vulnerability management and configuration management need improvement to ensure the confidentiality, integrity, and availability of University data and IT resources.

BACKGROUND

The University of Florida (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors (BOG). The University is directly governed by a Board of Trustees (Trustees) consisting of 13 members. The Governor appoints 6 citizen members and the BOG appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered 5-year terms. The Faculty Senate Chair and Student Body President also are members.

The BOG establishes the powers and duties of the Trustees. The Trustees are responsible for setting University policies, which provide governance in accordance with State law and BOG Regulations. The University President is selected by the Trustees and confirmed by the BOG. The University President serves as the Executive Officer and the Corporate Secretary of the Trustees and is responsible for administering the policies prescribed by the Trustees for the University.

The University uses the Oracle PeopleSoft Enterprise Applications (PeopleSoft) for the University's finance, human resources, and student applications. In addition, the University maintains and manages the network domain and IT infrastructure supporting PeopleSoft.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Awareness Training

A comprehensive security awareness training program instructing all employees on the importance of preserving the confidentiality, integrity, and availability of data and information technology (IT) resources entrusted to them is a foundational control for security vigilance and preventing and mitigating cybersecurity risks. An effective security awareness program includes identification of the specific

knowledge, skills, and abilities needed to support University security and educates all employees on how to interact with data and IT resources in a secure manner.

To evaluate University security awareness and skills training for University employees, we held discussions with University personnel and examined University records. We found that University Human Resources services used a learning management platform to assign applicable training, including security awareness training, to all University employees. The Information Security Office (ISO) within the University Central IT Division developed the University security awareness training, which addressed topics such as phishing, social engineering, restricted data, workspace and mobile device security, travel security, use of cloud and collaboration tools, and incident reporting.

According to University management, training is assigned for all employees with expected completion within 30 days from their hire date and, thereafter, training is expected every 12 months from the date of the previous training completion. The ISO tracked completion of security awareness training with reporting metrics provided to the University College and Administrative units responsible for reminding employees to complete the training; however, security awareness training was not required by University policies and University procedures had not been established to ensure that security training was completed.

As of March 7, 2025, 47 percent of University employees had not completed security awareness training. According to University personnel, each college or unit had the discretion to determine whether to enforce consequences for not completing the training. In response to our inquiry, University management indicated that the ISO and Office of Internal Audit continued to promote the importance of training completion for all employees through provision of training metrics to University management.

Effective security awareness training programs require completion by all employees. The lack of security awareness training increases the risk that employees may compromise the confidentiality, availability, and integrity of University data and IT resources.

Recommendation: To reduce cybersecurity risks, University management should establish security awareness training policies and procedures. Such policies and procedures should mandate timely completion of training by all employees and include enforcement measures for noncompliance.

Finding 2: Security Controls – Vulnerability Management and Configuration Management

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to vulnerability management and configuration management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of University data and related IT resources. However, we have notified appropriate University management of the two findings in the areas needing improvement.

Without appropriate security controls related to vulnerability management and configuration management, the risk is increased that the confidentiality, integrity, and availability of University data and related IT resources may be compromised.

Recommendation: We recommend that University management improve certain security controls related to vulnerability management and configuration management to ensure the confidentiality, integrity, and availability of University data and IT resources.

PRIOR AUDIT FOLLOW-UP

The University had taken corrective actions for the findings included in our report No. 2019-138.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this information technology (IT) operational audit from February 2025 through August 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected significant University IT controls applicable to Oracle PeopleSoft Enterprise Applications (PeopleSoft) and University IT infrastructure during the period June 2024 through May 2025, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were to:

- Evaluate the effectiveness of selected significant IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- Determine whether management had taken corrective actions for the findings included in our report No. 2019-138.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of and evaluating the IT systems and related significant controls; exercising professional judgment in

considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, and other guidelines to obtain an understanding of the University organizational structure and regulatory requirements and reviewed University procedures, interviewed University personnel, and examined University records to obtain an understanding of University operations related to PeopleSoft and IT infrastructure and to evaluate whether University operations were designed properly and operating effectively.
- Evaluated the effectiveness of University logical access controls assigned for the University network and selected network devices.
- Evaluated the effectiveness of logical access controls assigned for the supporting PeopleSoft infrastructure, including University procedures for the periodic evaluation of accounts assigned access privileges.
- Evaluated selected security settings related to PeopleSoft and the University network infrastructure to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Evaluated University procedures and examined selected scan reports and policies to evaluate the adequacy of University vulnerability management controls related to the IT infrastructure, including vulnerability assessment and remediation, malicious software identification, and malware defense.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges as of March 5, 2025, within the four default network administrator system groups for the University network domain.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges as of June 5, 2025, for the high risk network device for the University network.
- Examined and evaluated selected University patch management controls for operating systems and network devices to ensure that secure configurations are maintained. Specifically, we examined and evaluated:
 - As of March 4, 2025, 9 of the 75 critical application, Web, database, and identity and access management servers and 7 of the 92 critical network servers.
 - As of March 27, 2025, the one high risk network device for the University network.
- Evaluated the effectiveness of University configuration management controls, including those for establishing and maintaining secure configurations; disabling insecure protocols; implementing

firewalls or port filtering to protect network resources; and timely applying software patches and updates and managing device end-of-life.

- Evaluated the effectiveness of University security awareness training.
- Evaluated University procedures and examined selected records to determine the adequacy of University procedures for maintaining a software asset inventory and ensuring that only authorized software is installed on the network.
- Evaluated University procedures and examined selected backup reports to determine the adequacy of the University data recovery procedures to restore University IT assets to a pre-incident trusted state.
- Examined logging settings and related reports to determine the adequacy of University logging and monitoring controls designed for the University network and infrastructure supporting PeopleSoft.
- Examined and evaluated the appropriateness of all accounts assigned as of March 27, 2025, for the 62 critical application and Web servers supporting PeopleSoft.
- Evaluated University procedures and examined selected records to determine the adequacy of University procedures to enforce cybersecurity policies.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading **MANAGEMENT'S RESPONSE**.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.



Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

University of Florida Response: IT Operational Audit 2025

Finding 1: Security Awareness Training

Recommendation: To reduce cybersecurity risks, University management should establish security awareness training policies and procedures. Such policies and procedures should mandate timely completion of training by all employees and include measures for noncompliance.

Management's Response: As recommended, University of Florida Information Technology has reviewed current security policies and procedures and updated a draft Security Awareness Training policy to include the timely completion of training and measures for noncompliance. This draft update will now go through the University's policy review process.

Status: In Progress

Target Policy Publish Date: 12/31/2026

Responsible Party: University of Florida Information Technology

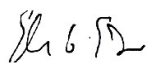
Finding 2: Security Controls – Vulnerability Management and Configuration Management

Recommendation: We recommend that University management improve certain security controls related to vulnerability management and configuration management to ensure the confidentiality, integrity, and availability of University data and IT resources.

Management's Response: As recommended, the University promptly addressed certain security controls related to vulnerability management and configuration management identified during the audit. The University has implemented a process to continuously review its security controls for vulnerability and configuration management as new risks are identified.

Status: Complete

Responsible Party: University of Florida Information Technology



Elias G. Eldayrie, UF Senior Vice President & Chief Information Officer
11/3/2025 | 6:57 PM EST